UNITED STATES PATENT APPLICATION

FOR

WIRELESS BRIDGE FOR ROAMING IN NETWORK ENVIRONMENT

Inventor(s):

Michael Wright
Douglas Hale
Anthony Jeffree
Peter Boucher

Sawyer Law Group LLP
2465 E. Bayshore Road, Suite 406
Palo Alto, California 94303

WIRELESS BRIDGE FOR ROAMING IN NETWORK ENVIRONMENT

FIELD OF THE INVENTION

The present invention relates to local area networks, and more particularly to roaming within local area networks.

BACKGROUND OF THE INVENTION

Figure 1 illustrates a conventional local area network (LAN). The LAN comprises a first bridge device 102, a second bridge device 104, and a mobile device 106 within the same bridging domain. The mobile device 106 can move from a connection with the first bridge device 102 at a first location in the network to a connection with the second bridge device 104 at a second location in the network. For example, the mobile device 106 can be a laptop computer. When at his original office location, a user connects the mobile device 106 to the LAN via the first bridge device 102. When the user moves to a new office, the mobile device 106 is connected to the LAN via the second bridge device 104. Existing standards, such as 802.1W, 802.1Q, and 802.1X, defined how this move is handled. Under these standards, the Media Access Layer (MAC) address of the mobile device 106 is maintained even as the it moves from the first 102 to the second 104 bridging devices. Because the MAC address of the mobile device 106 is maintained from the first location to the second location, the other devices in the network do not realize that the mobile device 106 has changed physical location. However, the routing of packets between the mobile device 106 and the network must be changed to ensure that packets are routed to the proper physical location. This is done through a "context" associated with the mobile device 106, which is

created by the first bridge device 102 when the mobile device 106 is connected to it.

The context comprises information such as the identity of the mobile device 106, how to maintain the status of a port to which the mobile device 106 is connected, the identity of the virtual LAN to which the mobile device 106 is connected, and how to return packets from the mobile device 106 to various locations throughout the LAN. Because the MAC address of the mobile device 106 is maintained within the same bridged domain under the standard, in order to ensure that packets are still properly routed to the mobile device 106 after it moves to the second bridge device 104, the context is transferred from the first bridge device 102 to the second bridge device 104. However, the context is typically transferred out-of-band, unsecurely, via a third party administrator. This conventional method of transferring the context creates a particularly significant security problem when the LAN is a wireless network because of the increased ease in interception and interjection of packets. Also, the conventional method is inefficient and cumbersome when a mobile device changes locations frequently, such as may be desirable for a wireless network.

Accordingly, there exists a need for an improved method for roaming in a network environment. The present invention addresses such a need.

SUMMARY OF THE INVENTION

The method for roaming in a network environment utilizes a token created by a first bridge device. The token comprises an identity of a context associated with the mobile device. The first bridge device creates the token and securely provides it to the mobile device. When the mobile device roams to a second bridge device in the network, the token is securely provided to the second bridge device. The second bridge device uses the token to

establish to the first bridge device that it is a genuine agent of the mobile device. Once the first bridge authenticates the second bridge device's authority, it securely sends the context associated with the mobile device to the second bridge device. The second bridge device uses the context to properly connect the mobile device to the network. In this manner, secure roaming within a bridged network is provided.

BRIEF DESCRIPTION OF THE FIGURES

Figure 1 illustrates a conventional local area network (LAN).

Figure 2 illustrates a preferred embodiment of a network environment in accordance with the present invention.

Figure 3 is a flowchart illustrating a preferred embodiment of a method for roaming in a network environment.

Figure 4 is a flowchart illustrating an example implementation of the preferred embodiment of the method for roaming in a network environment in accordance with the present invention.

DETAILED DESCRIPTION

The present invention provides an improved method for roaming in a network environment. The following description is presented to enable one of ordinary skill in the art to make and use the invention and is provided in the context of a patent application and its requirements. Various modifications to the preferred embodiment will be readily apparent to those skilled in the art and the generic principles herein may be applied to other embodiments. Thus, the present invention is not intended to be limited to the embodiment

shown but is to be accorded the widest scope consistent with the principles and features described herein.

The method in accordance with the present invention utilizes a "token" created by a first bridge device in the network. The token comprises an identity of a context associated with the mobile device when the mobile device is connected to the network through the first bridge device. The first bridge device creates the token and securely provides it to the mobile device. When the mobile device roams to a new location in the network comprising a second bridge device, the token is securely provided to the second bridge device. The second bridge device uses the token to establish to the first bridge device that it is a genuine agent of the mobile device. Once the first bridge authenticates the second bridge device's authority, it securely sends the context associated with the mobile device to the second bridge device. The second bridge device uses the context to properly connect the mobile device to the network at its new location.

To more particularly describe the features of the present invention, please refer to Figures 2 through 4 in conjunction with the discussion below.

Figure 2 illustrates a preferred embodiment of a network environment in accordance with the present invention. The network comprises a first bridge device 202 at a first location in the network, a second bridge device 204 at a second location, and a mobile device 206 which roams from the first bridge device 102 to the second bridge device 104. The mobile device 206 is originally connected to the network through the first bridge device 202. The mobile device 206 then roams to the second location and attempts to connect to the network through the second bridge device 204. In the preferred embodiment, the first 202 and the second 204 bridge devices are within the same bridged network. The preferred

embodiment utilizes a token 208 which comprises an identity of a context associated with the mobile device.

Figure 3 is a flowchart illustrating a preferred embodiment of a method for roaming in a network environment. First, the first bridge device 202 creates the token 208, via step 302. The token 208 is securely provided to the mobile device 206 by the first bridge device 202, via step 304. When the mobile device 206 roams and attempts to connect to the network through the second bridge device 204, the mobile device 206 securely provides the token 208 to the second bridge device 204, via step 306. By providing the token 208, the mobile device 206 gives the second bridge device 204 authority to act as its agent. The second bridge device 204 securely provides the token 208 to the first bridge device 202, via step 308, either directly or through at least one intermediary device (not shown). The first bridge device 202 authenticates the token 208 from the second bridge device 204, via step 310, to ensure that the token 208 is the one it original gave to the mobile device 206. Once the token 208 is authenticated, the context is securely provided by the first bridge device 202 to the second bridge device 204, via step 312, either directly or through at least one intermediary device. In this manner, secure roaming in a network environment is provided. The security is sufficient to support wireless roaming, where the mobile device 206 can frequently change locations.

"Security", as used in this specification, refers to the combination of secrecy and integrity. Secrecy refers to the ability to prevent an unauthorized party from obtaining data, even if a message containing the data is intercepted. Integrity refers to the ability to ensure that the content of the data is untampered. To be secure, a method should provide both secrecy and integrity.

Figure 4 is a flowchart illustrating an example implementation of the preferred embodiment of the method for roaming in a network environment in accordance with the present invention. In this implementation, the first bridge device 202, the second bridge device 204, and the mobile device 206 are each assigned their own public key/private key pairs. Public key/private key pairs, as used in cryptography, are well known in the art.

First, when the mobile device 206 is connected to the network through the first bridge device 202, the first bridge device 202 assigns an identifying number to the context associated with the mobile device 206, Cid, and creates messages A, B, and C. Message A is a nonce which is a first random number, R0, encrypted using the public key of the mobile device 206, via step 402. Message B is R0 and the Cid encrypted using the public key of the first bridge device 202, via step 404. In the preferred embodiment, message B is the mechanism by which the first bridge device 202 associates R0 with Cid without having to maintain its own copy of R0 and Cid. Alternatively, the first bridge device 202 can securely maintain its own copy of R0 and Cid in a storage medium, such as registers or random access memory (RAM). Message C is a digital signature for R0 and Cid, via step 406. In the preferred embodiment, the digital signature is an encrypted hash of R0 and Cid. The messages A, B, and C together comprise the token 208 as created by the first bridge device 202, via step 302 (Fig. 3).

The token 208 is then sent to the mobile device 206, via step 408. The encryption of messages A and B provide secrecy since only the intended recipient can decrypt the messages. The digital signature of message C provides integrity since only the original sender could have created the signature, and the signature will not match if the contents were modified. Therefore, the token 208 is securely provided to the mobile device 206 by the first

bridge device 202, via step 304 (Fig. 3).

When the mobile device 206 roams and connects to the second bridge device 204, the mobile device 206 first obtains R0 by decrypting message A using its own private key, via step 410. Only the mobile device 206 can decrypt message A since only it has the private key which matches the public key used to encrypt message A. The mobile device 206 then creates message D by encrypting R0 using the public key of the second bridge device 204, via step 412. Messages D, B, and C together now comprise the token 208. This token 208 is sent to the second bridge device 204, via step 414. The encryption of the messages D and B provide secrecy, and the digital signature of message C provides integrity. Therefore, the token 208 is securely provided to the second bridge device 204 by the mobile device 206, via step 306 (Fig. 3).

The second bridge device 204 obtains R0 by decrypting message D using its own private key, via step 416. The second bridge device 204 can decrypt message D since only it has the private key which matches the public key used to encrypt message D. The second bridge device 204 then creates message E, which is a new nonce which is a second random number, R1, encrypted using R0, via step 418. The second bridge device 204 also creates message F, which is R1 encrypted using the public key of the first bridge device 202, via step 420. Messages E, F, B, and C together now comprise the token 208. This token 208 is sent to the first bridge device 204, via step 422. The encryption of message E provides both secrecy and integrity, as described further below. The encryption of messages F and B also provide secrecy. The digital signature in message C provides integrity. Therefore, the token 208 is securely provided to the first bridge device 202 by the second bridge device 204, via step 308 (Fig. 3).

The first bridge device 202 recovers R1' by decrypting message F using its own private key, via step 424. R1' is the R1 recovered from message F. The first bridge device 202 then recovers its own version of R0 and Cid by decrypting message B using its own private key, via step 426. Only the first bridge device 202 can decrypt messages F and B because only it has the private key that matches the public key used to encrypt the messages. The first bridge device 202 also obtains R1 by decrypting message E using R0 obtained from message B, via step 428. If R1' = R1, via step 430, then the origin of token 208 from the second bridge device 204 is verified. R1' will equal R1 only if the R0 used to encrypt message E is the same as the first bridge device's version of R0. The first bridge device 202 knows that only it and the mobile device 206 had knowledge of R0. Thus, for the second bridge device 204 to be able to successfully encrypt message E with R0, it must have obtained R0 from the mobile device 206. The first bridge device 202 also verifies the digital signature in message C, via step 432. By verifying that R1' = R1 and verifying the digital signature, the token 208 from the second bridge device 204 is authenticated, via step 310 (Fig. 3). The second bridge device's 204 authority to act as the mobile device's 206 agent is thus established.

The first bridge device 202 then encrypts the context identified by Cid, i.e., the context associated with the mobile device 206, using R1, via step 434. The encrypted context is sent to the second bridge device 204, via step 436. The encryption of the context provides secrecy. Because only the first 202 and the second 204 bridge devices have knowledge of R1, encryption of the context with R1 also provides integrity. Therefore, the context is securely sent to the second bridge device 204, via step 312 (Fig. 3).

The second bridge device 204 decrypts the context using its own copy of R1. The

context is used to properly connect the mobile device 206 to the network at its new location. The second bridge device 204 then becomes the new first bridge device, creates a new token associated with the mobile device 206, and securely provides the new token to the mobile device 206.

An improved method for roaming in a network environment has been disclosed. The method utilizes a token created by a first bridge device. The token comprises an identity of a context associated with the mobile device when the mobile device is connected to the network through the first bridge device. The first bridge device creates the token and securely provides it to the mobile device. When the mobile device roams to a new location comprising a second bridge device in the network, the token is securely provided to the second bridge device. The second bridge device uses the token to establish to the first bridge device that it is a genuine agent of the mobile device. Once the first bridge authenticates the second bridge device's authority, it securely sends the context associated with the mobile device to the second bridge device. The second bridge device uses the context to properly connect the mobile device to the network at its new location. In this manner, secure roaming within a bridged network is provided.

Although the present invention has been described in accordance with the embodiments shown, one of ordinary skill in the art will readily recognize that there could be variations to the embodiments and those variations would be within the spirit and scope of the present invention. Accordingly, many modifications may be made by one of ordinary skill in the art without departing from the spirit and scope of the appended claims.